I-205

TICOM/I-205

DETAILED INTERROGATION REPORT OF FORMER
REGIERUNGSBAURAT JOHANNES ANTON MIRQUART
OF OKH/GEN d. NA.

Attached is the report of the detailed interrogations of former Regierungsbaurat Johannes Anton MIRQUART, head of Section 1a, Gruppe IV, General der Nachrichtenaufklaerung, carried out by Mr. K.L. PERRIN of L.S.I.C. and Captain Mary C. LANE of Army Security Agency, Europe, at Stuttgart on 9th and 10th June, 1947.

TICOM
20th June, 1947.

No. of Pages : 8

Copy No. : 22.

Distribution :-

L.S.I.C.

1. T
2. S
3. H
4. M
5. L
6. Z
7. H.71
8. H.62
9. H.63
10. L.91
11-14. Ticom Files.

U.S.L.O.

15. U.S.L.O.
16-19. OL-20-2.
20-23. A.S.A. Washington.
24. Director, A.S.A. Europe.

} via U.S.L.O.

External.

25. Signals 6, War Office.
26. D.S.D.10., Admiralty.
27. Signals 5, Air Ministry.

DETAILED INTERROGATION OF JOHANNES ANTON MARQUART, FORMER REGIERUNGSBAURAT AND HEAD OF REFERAT 1a OF GRUPPE IV, GENERAL DER NACHRICHTENAUFKLAERUNG, CARRIED OUT AT STUTTGART, GERMANY, ON 9-10TH JUNE, 1947, BY MR. K.L. PERRIN OF L.S.I.C. AND CAPTAIN MARY C. LANE, ARMY SECURITY AGENCY, EUROPE.

---

1. Career at OKH :

JOHANNES ANTON MARQUART was posted to OKH/In 7/IV as an Angestellter in 1940, and for the first year carried out research on German hand systems. In 1941 he was transferred to In 7/VI and, with the rank of Sonderfuehrer (Z), was put in charge of a series of courses in elementary cryptanalysis, which work he continued until 1944. He was then promoted Regierungsbaurat and was given command over Section 1a for special research on hand cyphers. His experience of practical cryptanalysis is therefore confined to hand systems which appeared during the last part of the war. During this period he worked under PIETSCH while similar work on machine systems was carried out by DOERING, head of Section 1b.

2. Cryptanalytic Experience :

As head of the special research section for hand cyphers Marquart's work was of a varied nature; and he was asked to give an account of the specific tasks which had fallen to his lot.

a. Tito System : This consisted of the alphabet substituted into figures in such a way that the commonest letters were allotted one figure equivalents while the rarer letters were expressed as figure digraphs. The resulting figures were then recyphered by a periodic additive, the length of which varied from time to time. At first the period was very short (5, 7 or 9); later it rose to 35 or 45, and at the end MARQUART thought that it was used on a one-time basis, since no further success could be achieved.

b. Mihailovic System : This was Double Transposition, using the same key for both cages, the keys being derived from a novel. MARQUART's section achieved a fair measure of success with this system,,owing to errors in encypherment, stereotyped signatures, and also the fact that the cages were often filled up to rectangles with rare letters. Under such circumstances it was often possible to recover the key from a single message. In some cases, by working out the basic text from which the keys had been derived, they were able to recognise and obtain the novel and thence to read all traffic currently. All cryptanalytic work on double transposition systems was carried out entirely by hand and no attempt was made to develop any statistical machine method of solution.

c. British Army Double Transposition : This presented a considerably more formidable task, since two different keys were used which were taken from a large book. MARQUART was unable to guess at the size of the book, since it had never been captured, and their only guide was a captured copy of the instructions. Their work consisted of looking for errors in encypherment which happened but rarely, and for messages in depth which practically never occurred. When a message was broken by these means, the Germans were thus provided with two keys from the book; they could then take any message having one of these as the first decypher key and, by thus reducing the problem to one of single transposition, could recover the second decypher key. However, they never succeeded in breaking messages in which only the second decypher key was known. MARQUART estimated that only about one message in a thousand could be read in this way and that altogether they had recovered less than 100 keys. He was not aware that this system had ever been replaced by another in the British Army.

d. Russian "Blocknots". MARQUART's section was given the task of making a research into the Russian "blocknot" traffic. A considerable number of original key-pages had fallen into German hands. The problem could be divided into "individual Blocknots" and "general Blocknots". The "individual Blocknots" consisted of small pads of key-pages, each consisting of 50 or 60 five-figure groups (he was not sure which). In theory, each page was used for only one

Please turn over

message and was torn off immediately after use. In practice, however, when supplies were running low, the last pages tended to be used several times, and in these cases the Germans were able to read the messages.

"General Blocknots" were much larger, consisting of 31 pages, each containing 30 lines of 10 five-figure groups. Along the top were the numbers 0 - 9 in natted order, indicating the ten columns. Down the side, the rows were indicated by a random selection of three-figure numbers. Each page was used for one day only and the p ds were changed monthly. At first, solution of these was very easy, since all messages began at the top left-hand corner; then they began to use the beginning of any row, and finally any group on the page could be the starting-point. This was indicated by a five-figure group, consisting of the three figures representing the row, followed by the figure representing the column, and one dummy figure. At first, this indicator was recyphered merely by adding the figures to those of the first group of the cypher text; later, however, the indicator recyphering system became much more complicated, the Germans were unable to break it, and MARQUART could not describe the system involved.

With the introduction of the new indicator recyphering system towards the end of the war, the setting of messages in depth and solution of the additive became much more difficult, and their success was spasmodic according to the volume of traffic. Hollerith machinery was used for this task. They were considerably aided by the fact that the Russians tended to choose starting-points from the first three rows of the page. Encyphering was done cyclically, i.e. if the encypherer reached the bottom of the page he then carried on at the top.

The underlying book consisted of a five-figure alphabetical code which was quite easy to solve. Even when the Russians knew that the basic book was compromised, they did not bother to change it, but relied upon the additive for the security of the system.

On the basis of the "Blocknots" which had been captured, MARQUART's section carried out an intensive research in an attempt to discover the method by which they were produced. All the counts which they made, however, failed to reveal any non-random characteristics in the make-up of the tables, and while they thought that the "Blocknots" must be made by machine, they were never able to draw any concrete deductions as a result of their research. (In this connection MARQUART said that this was the only case in which such a research had been made, since nowhere else was there sufficient captured material upon which to work). Occasionally, however, they had found the same table of figures with two different pad numbers, but they could not establish whether this was due to an error in compilation or to a fault in the method of production.

e. Polish Lublin System : Lastly, MARQUART described the work which he had done on a system used by the military forces of the Lublin Government just before the end of the war. The Germans had never discovered the complete method of operation of this system, and MARQUART was somewhat vague about some of the details. After some difficulty, however, the interrogators managed to extract sufficient information to piece together the principle on which the system worked.

The Poles employed a considerable number of keys, consisting of the numbers 0 - 9 in natted order. The key to be used for the message was determined by the indicator, about which, however, MARQUART was unable to give any details. The key selected was written out three consecutive times on a strip. A second strip consisted of the alphabet, probably in normal order. Thirty positions were available on this strip, but MARQUART could not remember whether the extra four spaces were given up to accented letters or to punctuation. The alphabet strip was also marked with an arrow to indicate the position in which the key strip was to be set.

Encyphering consisted of changing letter digraphs into figure trigraphs by the following method: for the first digraph, number one on the key strip was set opposite the arrow on the alphabet strip, and the encypherer then read the two figures corresponding to the letters of the digraph. Since, however, each number on the key strip represented three letters on the alphabet strip, a third figure was required to indicate which of the three possible letters was intended. A small table was therefore provided in which each of the possible combinations of the three positions was represented by a number. For example, if the first letter of the digraph was taken from the third part of the alphabet, and the second letter of the digraph from the first part, then the encypherer would look up the combination III,I on the table, and if he found that it was represented by the number eight, he would prefix this number to those which he had already obtained by substitution.

Please turn over

The encypherer would then move the key-strip until the number two appeared opposite the arrow on the alphabet strip and would then proceed with the substitution of the second digraph of the plain text. Similarly, he would continue throughout the ten numbers of the key in numerical order. The eleventh digraph would then be encyphered on the same substitution as the first, the twelfth on the same substitution as the second etc.

MARQUART's example of this system is as follows :-

Polnisches Heeresverfahren 1945

```
   3 7 2 5                                                          Lage 3
3 7 2 5 8 4 | 6 9 1 0 3 7 2 5 8 4 | 6 9 1 0 3 7 2 5 8 4 6 9 1 0 3 7 ...  Lage 2
| 6 9 1 0 3 7 2 5 8 4 6 9 1 0 3 7 2 5 8 4 6 9 1 0 3 7 2 5 8 4 | . . . . .  Lage 1
a b c d e f g h i j | k l m n o p q r s t | u v w x y z (.) (,) | a b c d
      |       I     |          II         |          III        |    I
```

fu	nk	sp	ru	ch
176	353			

I,I	6
I,II	9
I,III	1
II,I	0
II,II	3
II,III	7
III,I	8
III,II	5
III,III	2,4

From the cryptanalytic point of view, the characteristics of this system were as follows :-

(i) Since there were only nine combinations of the three parts of the alphabet, it followed that in a particular key, either one number could never appear as the first figure of a trigraph, or, if two figures were allotted to a particular combination, these two figures would appear less frequently than the rest. (MARQUART was not clear which of these two conditions obtained).

(ii) If messages were written out on a period of 30, there would be a marked frequency distribution in each column of trigraphs.

MARQUART stated that this system was broken too late to be of any practical importance.

3. OKH Cryptanalysis :

Except for the subjects listed above, MARQUART's knowledge of the cryptanaltyic work of OKH was based upon what he was told by the other members and is therefore of a very general nature.

a. British Systems : The head of the English Referat was Oberinspektor ZILLMANN (fnu) about whom MARQUART had not heard since the end of the war. MARQUART mentioned first the work which had been done on Typex in 1940/41 and described briefly how they had made a study of the indicators and on the basis of bad usage had found out a certain amount concerning the working of the machine, the period of the wheels, etc. Their conclusions had been confirmed when they were given the opportunity to inspect a captured machine which had been lying in OKW for six months without their knowledge. He believed that this machine had been captured in France. The wheels were missing and never in the course of the whole war did they succeed in capturing any wheels. They reached the conclusion in 1941 that there was no possibility of success without the wheel wirings. They therefore abandoned all work on this system except for a routine watch on the traffic. (Note: MARQUART was not pressed for details since these are to be found in the recently discovered OKH documents). He said that they never had any cribs of Typex messages on which to work.

MARQUART was extremely vague on the subject of British additive systems. He had a vague recollection of War Office Cipher which he thought was read on depths in the early years of the war. After about 1942 all attempts to find repeats by Hollerith methods failed and they came to the conclusion that each

Please turn over

message must have a different key. Attempts to set messages in depth continued throughout but with no success. He did not recollect any other British additive system.

The only other British systems about which he knew besides the double transposition which has been described above (para 2c) were daily changing unreciphered three-letter codes which were used in Africa about 1944 and read fairly regularly when sufficient depths were available, and Slidex which was read consistently until the end of the war.

b. American Systems : The head of the American Section was Friedrich STEINBERG from whom MARQUART had not heard since the end of the war. The first American cipher to be broken by OKH was the 25 strip system. MARQUART described the gradual stages by which the principle was recovered. First they found repeats at the beginnings of messages and then repeats at intervals (getrennte Serien) on a period of 25. When they had accumulated depth up to 20 they were able to solve individual messages and found them to be based upon 25 substitution alphabets. It was only after they had solved a number of keys that they found the relationship among the various messages and were able to read the rest of the traffic. MARQUART mentioned that they were greatly assisted in recognising the system by a description which they read in a book published in the United States just before the war. He could not remember the name of the publication and thought it might conceivably have been a private brochure. It was not the Black Chamber. This system was not broken for very long before it changed and they no longer found any repeats.

They also read some three-letter codes which at first were used unrecyphered, and subsequently were recyphered by conversion tables. He expressed the opinion that these tables might not have been broken if they had not first been able to break the basic code while it was still unrecyphered.

MARQUART spoke briefly of the solution of the M-209 by errors in encypherment and messages in depth which enabled them to work out the periods and pin-settings. He said that they never had a captured machine, nor did they ever get cribs on which to work.

He had not heard of any other American machine, and did not recognise the term "big American machine" or the discriminant DOLOF.

c. Russian Systems : MARQUART stated that at one time they had captured a small Russian machine; he thought it was electric but did not know the principle and was unable to describeit. No traffic was ever intercepted on this system but it could certainly have been solved with a small amount of material.

All other Russian systems known to MARQUART were hand systems, the principal one being the "Blocknots" described above (para 2 d). During the greater part of the war all work on Russian systems was carried on very successfully by the out-stations, and he was therefore unable to give many details. He knew that they consisted mainly of three- and four-figure alphabetical codes recyphered in various ways by conversion tables. Many of the Russian divisions were provided with a basic key square composed of 10 rows and 10 columns of the numbers 0 - 9 hatted. By juggling with rows and columns in various ways the Russians were able to derive a considerable number of 10 figure keys for use as conversion tables. In many cases the Germanswere able to see the relationship between the keys which they had reconstructed and at least partially to recover the basic key square.

MARQUART stressed that the production of Russian cyphers was completely decentralised and was generally carried out divisional level, and each division therefore had its own favourite methods of key production. Not all divisions used the basic key squares described in the above paragraph. He thought, however, that the high grade Russian systems such as the "Blocknots" were probably produced by the central authority. He considered that decentralised production, while it presented a greater variety of methods to the enemy cryptanalyst, was an undesirable system in that it necessitated the presence of experiencedofficers at divisional level to oversee the work.

MARQUART also mentioned a two-figure system in which the call-signs were encyphered on the same conversion table as the messages. Each station was provided with a basic call-sign consisting of a two-figure number, and each day this number was looked up on the 10 x 10 square and recyphered by the vertical and horizontal keys. By following the call-signs from day to day the work of recovering the daily changing keys was considerably facilitated. MARQUART stated that this was done because the Russians employed only figure cyphers and their operators never learned letter Morse and therefore were unable to cope with letter call-signs. He insisted that no letter cypher of any kind was ever used by the Russians.

d. Other Countries and Systems:

(1) Hungary : Like the Croations, the Hungarians were provided with their Enigma wheel wirings by a German firm and these were therefore available to OKH. They were thus able to read the traffic.

(2) Croatia : MARQUART said that the solution of the Croatian Enigma was facilitated because it had no stecker. While he was unwilling to commit himself, he thought it possible that the Germans would have been unable to read the Enigma with stecker even though they had the wheel wirings.

(3) Poland : He knew nothing about the Polish systems solved at the beginning of the war. The Germans only began to study Polish again towards the end and the system described above (para 2 c) was the main one employed. He thought there might have been other systems but was unable to give details.

(4) Finland : There was no Finnish Referat in OKH and Finnish systems were never studied.

(5) France : MARQUART claimed to know very little about French cyphers other than the fact that the C-36 was captured after the fall of Paris. He stated that as he was resident in the French Zone of Germany he was unwilling to give information on this subject, and the matter was not pressed.

(6) Agents' Systems : MARQUART was unaware that these had been studied at OKH. He said that VAUCK had attended one of his courses, but that he had subsequently been transferred to OKW. MARQUART had never heard of Referat 12.

(7) Teleprinter Systems : He reiterated that he knew nothing at all about the technicalities of this subject and that DOERING was the expert on all machine matters. He thought that Hauptmann ROEDER had also been responsible for teleprinter systems. He know that they had had considerable difficulty in intercepting such traffic and thought that the underlying text was only read when it was in the clear. He never heard of any such machine being captured.

(8) Call-sign Systems : He knew nothing at all about British call-sign systems since these had been studied in the traffic analysis group. He knew that the Russian call-sign systems were comparatively simple and were solved by the out-stations but he was unable to give any details.

4. Drvar Cave Incident :

At first MARQUART denied all knowledge of this episode. Later, however, he recalled that certain material had been discovered in a cave in Yugoslavia although he did not remember the name. The material was found by chance when some German soldiers entered a cave - he does not know how they came to be there - saw some papers lying on the ground and recognised them as cypher material. There was not a great deal of material and it was contained in one or two folders. It consisted entirely of cypher keys in several copies ready to be distributed to users. Since the documents fell into German hands they were naturally neither distributed nor used and he did not think they provided OKH with any important information. He thought that the papers had almost certainly been destroyed at Jueterbog at the end of the war along with all other useless documents.

5. NFAK 621 :

MARQUART was unable to distinguish between NFAK and NAK, nor had he ever heard of Company 621. However, he remembered that there had been an out-station at Tobruk which had worked mainly on two-letter codes and double transposition of the British Army. He was certain that they had had no machinery. Inspektor HARMS had been the first to go out there and later his place was taken by LIEDTKE who had been taken prisoner with his whole company. Immediately after this the British had changed all their systems. MARQUART knew of a Sergeant WAGNER who had been employed in Berlin at the beginning of the war, but did not think he had ever gone to Africa and knew of nobody of that name in Tobruk.

Please turn over

6. Liaison with other Bureaux :

MARQUART reiterated that liaison with other German bureaux except on German systems was not good. He claimed that he had never heard of the Forschungsamt and said that in any case he himself had not been concerned with any outside liaison.

He know that OKH had close liaison with Finland on Russian systems and there had been a Finnish liaison officer whose name he did not know at their outstation in East Prussia. Amongst other Russian systems they had exchanged all information concerning "Blocknots". The Finnish officer never came to Berlin.

He knew of no liaison with Hungary or Japan and thought that connections with Italy were very weak, although an Italian officer had once paid him a visit and he had been instructed to answer the Italian's questions in the most general terms.

He know nothing at all of any enemy cryptanalytic centres; the only prisoners whom they interrogated were wireless operators who were unable to give them any useful information.

7. German Systems :

From 1940 to 1941 MARQUART helped PIETSCH with the development of German hand systems. At that time the German Army was using double transposition (Heftschluessel) which they knew from captured documents had been read by the Poles. He thought that no Polish cryptanalysts had been apprehended and did not remember any reference in the documents to the German Enigma, and did not recognise the term Fall Wicher.

He knew LENZER faintly and thought that he had spent most of his time developing a new Hagelin machine which was never ready for use. He had never heard of the Schluesselschiebe or Schluesselkasten.

8. Hollerith Machinery :

The only cryptanalytic aids at their disposal were Hollerith machines which were used for finding repeats, depths, etc. At the end of the war they had intended to move the machines to Bad Reichenhall with their documents; they were dispatched on a train from Erfurt to Rosenheim and he does not know whether they ever arrived.

9. Cryptanalytic Courses :

From 1941 to 1944 MARQUART was in charge of a series of courses in elementary cryptanalysis which were given to all newcomers. The length of the course was six weeks or in urgent cases four to five weeks. The course dealt with the elementary principles of substitution and transposition, recyphered and unrecyphered codes, conversion tables, additives, etc. Most of the text books at their disposal were of French origin and included Baudouin, Cartier and Geviège. They also possessed a copy of Yardley's Black Chamber.

10. General Remarks :

MARQUART stated that his own special research section can hardly be considered to have been a success. Most of their problems were those which had been rejected by the country sections and the solution of the Lublin system came too late to have been of any practical importance. He was equally lugubrious about the general work of In 7/VI and said that they suffered from a very bad organisation for passing back intercepted material to the centre. Traffic generally arrived with a considerable time lag and results were obtained too late to be of any but strategic value. The bulk of the work was done by the outstations which coped very successfully with low grade systems. Their section in Berlin only received reports from the out-stations about once in three months and was therefore always out of touch with the latest developments. The most successful of the out-stations were those engaged on the Eastern front.

Please turn over

Most of their reports were not distributed outside OKH except in the case of work on their own systems and reports which were sent to the interested out-station. He himself had not written many reports since for the greater part of the war he had been occupied with running the cryptanalytic courses.

LAROUART was difficult to interrogate since he would only talk when prompted with specific questions. The interrogators consider, however, that he was probably telling most of what he knew and doubt whether any further information of value could be obtained. Most of his statements are confirmed and in much greater detail by the recently found OKH documents. It was considered advisable not to let LAROUART know that these were in our hands.